



PATRICK D. CROCKER
patrick@crockerlawfirm.com

February 27, 2009

Ms. Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

Filed Electronically Via ECFS

RE: Zenk Group, LTD d/b/a Planet Access
Customer Proprietary Network Information Certification
EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to 47 C.F.R. 64.2009(e) please find attached the 2008 Annual CPNI Certification and Accompanying Statement filed on behalf of Zenk Group, LTD d/b/a Planet Access.

Please contact the undersigned should you have any questions or concerns at (269) 381-8893 or patrick@crockerlawfirm.com.

Very truly yours,

CROCKER & CROCKER, P.C.


Patrick D. Crocker

PDC/tld

cc: FCC Enforcement Bureau (2 copies via USPS Mail)
Best Copy and Print, Inc. (via e-mail FCC@BCPIWEB.COM)

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: February 27, 2009

Name of Company Covered by this Certification: Zenk Group, LTD
d/b/a Planet Access

Form 499 Filer ID: 823172

Name of Signatory: Michael Zengerle


Title of Signatory: President

I am the President of Zenk Group, LTD d/b/a Planet Access and as such do hereby certify, affirm, depose, and say that I have authority to make this Customer Proprietary Network Information ("CPNI") Annual Certification of Compliance on behalf of Zenk Group, LTD d/b/a Planet Access I have personal knowledge that Zenk Group, LTD d/b/a Planet Access has established adequate operating procedures to ensure compliance with the Commission's CPNI rules as set forth in 47 C.F.R. § 64.2001 et. seq.

Attached to this Certification is an Accompanying Statement explaining how the company's procedures ensure compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

Zenk Group, LTD d/b/a Planet Access received no customer complaints in the past year concerning the unauthorized release of CPNI. Further, Zenk Group, LTD d/b/a Planet Access has taken no action against data brokers for the unauthorized release of CPNI during calendar year 2008. Zenk Group, LTD d/b/a Planet Access will report any information it may obtain with respect to the processes pretexters are using to attempt to access CPNI and what steps Zenk Group, LTD d/b/a Planet Access is taking to protect CPNI.

This certification is dated this 27 day of February, 2009.


Michael Zengerle
President
Zenk Group, LTD d/b/a Planet Access

Customer Proprietary Network Information Certification Accompanying Statement

ZENK GROUP, LTD d/b/a Planet Access ("ZENK") has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("FCC") rules pertaining to customer proprietary network information ("CPNI") set forth in sections 64.2001 — 64.2011 of the Commission's rules. This attachment summarizes ZENK's practices and procedures, which have been updated to adequately ensure compliance with the Commission's CPNI rules.

Safeguarding against pretexting

- ZENK takes reasonable measures to protect CPNI and believes that these measures sufficiently prevent unauthorized access to CPNI.

Training and discipline

- ZENK has trained its personnel in the appropriate use of CPNI. All employees with access to CPNI are required to review and comply with ZENK's CPNI policies and procedures.
- ZENK has disciplinary process in place for violations of ZENK's CPNI policies and procedures which would encompass any misuse of CPNI.

ZENK'S use of CPNI

- ZENK does not share, disclose, or otherwise provide CPNI to third parties.
- ZENK may use CPNI for the following purposes:
 - > To initiate, render, maintain, repair, bill and collect for services;
 - > To protect its property rights; or to protect its subscribers or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services;
 - > To provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent; and
 - > To market additional services to customers that are within the same categories of service to which the customer already subscribes.
- ZENK does not disclose or permit access to CPNI to track customers that call competing service providers.
- ZENK discloses and permits access to CPNI where required by law (e.g., under a lawfully issued subpoena).

Customer approval and informed consent

- ZENK does not use CPNI for any purpose that would require customer approval to do so. ZENK does not use CPNI for any marketing purposes and does not share, disclose, or otherwise provide CPNI to any third party. If this policy changes in the future, ZENK will implement practices and procedures to ensure compliance with the Commission's CPNI regulations.

Additional safeguards

- ZENK has established a supervisory review process designed to ensure compliance with the FCC's CPNI rules.
- ZENK designates one or more officers, as an agent or agents of the company, to sign and file a CPNI Compliance Certificate on an annual basis. The Certificate conforms to the requirements set forth in FCC rule 64.2009(e).
- ZENK properly authenticates a customer prior to disclosing CPNI based on customer initiated telephone contact, online account access, or an in-person visit.
- ZENK notifies customers immediately of any account changes.
- ZENK may negotiate alternative authentication procedures for services that ZENK provides to business customers that have both a dedicated account representative and a contract that specifically addresses ZENK's protection of CPNI.
- In the event of a breach of CPNI, ZENK will notify law enforcement as soon as practicable and no later than seven (7) business days from discovering the breach. Customers will be notified after the seven (7) day period, unless the relevant investigatory party directs ZENK to delay notification, or ZENK and the investigatory party agree to an earlier notification. ZENK will maintain a record of all CPNI security breaches, including a description of the breach and the CPNI involved, along with notifications sent to law enforcement and affected customers.